



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/944,996	08/31/2001	Brian K. Martin	RSW920010151US1	1846

46320 7590 05/31/2006

CAREY, RODRIGUEZ, GREENBERG & PAUL, LLP
STEVEN M. GREENBERG
1300 CORPORATE CENTER WAY
SUITE 105G
WELLINGTON, FL 33414

EXAMINER

HA, LEYNNA A

ART UNIT PAPER NUMBER

2135

DATE MAILED: 05/31/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

09/944,996

Applicant(s)

MARTIN, BRIAN K.

Examiner

LEYNNA T. HA

Art Unit

2135

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 23 February 2006.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-13 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-13 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

1. Claims 1-13 is pending.
2. This is a Non-Final rejection.

3. In view of the Appeal filed on February 22, 2005, PROSECUTION IS HEREBY REOPENED. The Non-Final rejection is set forth below.

To avoid abandonment of the application, appellant must exercise one of the following two options:

(1) file a reply under 37 CFR 1.111 (if this Office action is non-final) or a reply under 37 CFR 1.113 (if this Office action is final); or,

(2) request reinstatement of the appeal.

If reinstatement of the appeal is requested, such request must be accompanied by a supplemental appeal brief, but no new amendments, affidavits (37 CFR 1.130, 1.131 or 1.132) or other evidence are permitted. See 37 CFR 1.193(b)(2).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

4. Claims 1-9 and 11-13 are rejected under 35 U.S.C. 103(a) as being unpatentable over Rothermel, et al. (US 6,678,827), and further in view of Kikuchi, et al. (US 6,377,948).

As per claim 1:

Rothermel, et al. discloses a stealth firewall comprising:

a first network interface to an external network; **(col.1, lines 23-29)**

a second network interface to an internal network; **(col.1, lines 30-35 and col.11, lines 18-38)**

a packet filter for restricting access to said internal network; **(col.3, lines 4-8 and col.4, lines 53-54)**

a state machine **(col.4, lines 33-35)** pre-configured to transition across a plurality of internal states **(col.4, lines 35-45 and col.5, line 65 – col.6, line 2)**, from a restricting state to an access state **(col.15, lines 48-56 and col.13, lines 47-67)**,
[conditioned upon receiving a plurality of requests to access said internal network, said plurality of requests collectively comprising a code for causing said state machine to

Art Unit: 2135

transition from said restricting state to said access state] which causes said packet filter to permit access to said internal network; wherein **(col.11, lines 10-15)**

said packet filter not responding to said external network upon receiving any requests from said external network to access said internal network when said state machine in said restricting state. **(col.5, lines 39-51 and col.9, lines 28-39)**

Rothermel teaches messages can include a variety of types of requests (col.18, lines 1-8), and further discloses gathering network security information of activities where it is analyzed during the process of protection from unauthorized access (col.5, lines 30-35 and 55-63). However, did not discuss in further details the gathering of security information whereby receiving a plurality of requests to access said internal network, said plurality of requests collectively comprising a code for causing said state machine to transition from said restricting state to said access state.

Kikuchi an invention of transmitting and requesting access to documents on workstations through a network such as LAN (col.1, lines 12-15). Kikuchi discloses receiving a request for accessing information and analyzing the contents of the access request where the sequence of issued access requests are collectively reflected in the database as a single transaction (col.4, lines 15-22). In addition, when the client issues a sequence of access requests, the consistency is guaranteed for a plurality of information items to be process by the access requests (col.2, lines 62-65).

Hence, it would have been obvious for a person of ordinary skills in the art at the time of the invention to combine the method as taught by Kikuchi because by receiving a plurality of requests to access said internal network, said plurality of requests

Art Unit: 2135

collectively comprising a code for causing said state machine to transition from said restricting state to said access state guarantees for a plurality of information items to be processed, thus, can determine the restricting state to an access state of Rothermel.

As per claim 2: See col.2, lines 5-8; discussing requests from said external network comprise transport control protocol (TCP) SYN messages.

As per claim 3: See col.2, lines 5-8; discussing each state in said state machine corresponds to data in a specified field of said TCP SYN messages.

As per claim 4: See col.12, lines 1-2 and 60-64; discussing specified field comprises a destination port field.

As per claim 5: See col.8, lines 59-60; discussing code is a rolling code which can vary according to time.

As per claim 6: See col.5, line 65 – col.6, line 2 and col.11, lines 10-15; discussing packet filter can permit access to a specific port in said internal network based upon a destination port specified in a TCP SYN message received after transitioning to said access state in said state machine.

As per claim 7:

Rothermel discloses a method for permitting access to a network protected behind a stealth firewall comprising the steps of:

initializing a state machine (**col.4, lines 33-35**) configured to grant access to the stealth firewall contingent upon said state machine transitioning across a plurality of internal states responsive to (**col.4, lines 35-45**) *[receiving a plurality of requests to*

Art Unit: 2135

access the network from a single network device, said plurality of requests collectively comprising a code for causing said state machine to permit access to the network];

receiving an access request (col.17, lines 23-28 and col.18, lines 3-8) from a network device in a network which is external to the network protected behind the stealth firewall (col.1, lines 23-35 and col.11, lines 18-38), identifying an access parameter in said access request and transitioning from an initial state in said state machine to an intermediate state if said identified access request satisfies transitioning criteria associated with said state machine for transitioning from said initial state to said intermediate state; (col.8, lines 59-60 and col.13, lines 47-67)

[receiving a further access request from said network device in said network which is external to the network protected behind the stealth firewall, identifying a further access parameter in said further access request and transitioning from an intermediate state in said state machine to a final state if said identified further access request satisfies transitioning criteria associated with said state machine for transitioning from an intermediate state to said final state];

not providing a response to said network device upon receiving each said access request from said network device in said network which is external to the network protected behind the stealth firewall unless said network device (col.5, lines 39-51 and col.9, lines 28-39) [provides a sequence of access requests to the stealth firewall causing said state machine to transition to said final state]; and

upon transitioning to said final state, permitting said network device to access the network protected behind the stealth firewall. (col.5, line 65 – col.6, line 2 and col.11, lines 10-15)

Rothermel teaches messages can include a variety of types of requests (col.18, lines 1-8), and further discloses gathering network security information of activities where it is analyzed during the process of protection from unauthorized access (col.5, lines 30-35 and 55-63). However, did not discuss in further details the gathering of security information that includes receiving a plurality of requests to access the network from a single network device, said plurality of requests collectively comprising a code for causing said state machine to permit access to the network and receiving a further access request from said network device in said network which is external to the network protected behind the stealth firewall, identifying a further access parameter in said further access request and transitioning from an intermediate state in said state machine to a final state if said identified further access request satisfies transitioning criteria associated with said state machine for transitioning from an intermediate state to said final state whereby provides a sequence of access requests to the stealth firewall causing said state machine to transition to said final state.

Kikuchi an invention of transmitting and requesting access to documents on workstations through a network such as LAN (col.1, lines 12-15). Kikuchi discloses receiving a request for accessing information and analyzing the contents of the access request where the sequence of issued access requests are collectively reflected in the database as a single transaction (col.4, lines 15-22). In addition, when the client issues

Art Unit: 2135

a sequence of access requests, the consistency is guaranteed for a plurality of information items to be process by the access requests (col.2, lines 62-65).

Hence, it would have been obvious for a person of ordinary skills in the art at the time of the invention to combine the method as taught by Kikuchi because by receiving a plurality of requests to access said internal network, said plurality of requests collectively comprising a code for causing said state machine to transition from said restricting state to said access state guarantees for a plurality of information items to be processed, thus, can determine the restricting state to an access state of Rothermel.

As per claim 8:

Rothermel discloses a method for permitting access to a network protected behind a stealth firewall comprising the steps of:

[receiving a plurality of access requests] from a plurality of network devices **(col.1, lines 23-27)** which are external to the network protected behind the stealth firewall; **(col.1, lines 30-35 and col.11, lines 18-38)**

not providing a response to said plurality of network device upon receiving each of said access requests; **(col.5, lines 39-51 and col.9, lines 28-39)**

identifying access request parameters in said received access requests; **(col.5, line 63 – col.6, line 2)**

performing state transitions in a state machine in the stealth firewall based upon identifying particular ones of said identified access request parameters; *and*, **(col.11, line 64 – col.12, line 4 and col.12, lines 54-67)**

[upon identifying a pre-determined sequence of access request parameters, said identification of said sequence of access request parameters causing a corresponding sequence of state transitions in the said machine, permitting access to a selected network device responsible for transmitting said sequence of access requests parameters].

Rothermel teaches messages can include a variety of types of requests (col.18, lines 1-8), and further discloses gathering network security information of activities where it is analyzed during the process of protection from unauthorized access (col.5, lines 30-35 and 55-63). However, did not discuss in further details upon identifying a pre-determined sequence of access request parameters, said identification of said sequence of access request parameters causing a corresponding sequence of state transitions in the said machine, permitting access to a selected network device responsible for transmitting said sequence of access requests parameters.

Kikuchi an invention of transmitting and requesting access to documents on workstations through a network such as LAN (col.1, lines 12-15). Kikuchi discloses receiving a request for accessing information and analyzing the contents of the access request where the sequence of issued access requests are collectively reflected in the database as a single transaction (col.4, lines 15-22). In addition, when the client issues a sequence of access requests, the consistency is guaranteed for a plurality of information items to be process by the access requests (col.2, lines 62-65).

Hence, it would have been obvious for a person of ordinary skills in the art at the time of the invention to combine the method of receiving a plurality of access requests

Art Unit: 2135

whereby performing state transitions in a state machine in the stealth firewall based upon identifying particular ones of said identified access request parameters and upon identifying a pre-determined sequence of access request parameters, said identification of said sequence of access request parameters causing a corresponding sequence of state transitions in the said machine, permitting access to a selected network device responsible for transmitting said sequence of access requests parameters as taught by Kikuchi because this guarantees for a plurality of information items to be processed, thus, can determine the restricting state to an access state of Rothermel.

As per claim 9:

Rothermel discloses a method for permitting access to a network protected behind a stealth firewall comprising the steps of:

configuring a state machine to grant access to the stealth firewall contingent upon said state machine transitioning through a plurality of states *[based upon a sequence of access request parameters identified in received access requests]* from a single network device; **(col.1, lines 30-35 and col.11, lines 18-38)**

setting said sequence of access parameters to a specific set of access parameters; and, **(col.5, line 63 – col.6, line 2)**

disposing said state machine in the stealth firewall. **(col.12, lines 59-60)**

Rothermel teaches messages can include a variety of types of requests (col.18, lines 1-8), and further discloses gathering network security information of activities where it is analyzed during the process of protection from unauthorized access (col.5,

lines 30-35 and 55-63). However, did not discuss in further details based upon a sequence of access request parameters identified in received access requests.

Kikuchi an invention of transmitting and requesting access to documents on workstations through a network such as LAN (col.1, lines 12-15). Kikuchi discloses receiving a request for accessing information and analyzing the contents of the access request where the sequence of issued access requests are collectively reflected in the database as a single transaction (col.4, lines 15-22). In addition, when the client issues a sequence of access requests, the consistency is guaranteed for a plurality of information items to be process by the access requests (col.2, lines 62-65).

Hence, it would have been obvious for a person of ordinary skills in the art at the time of the invention to combine the method of based upon a sequence of access request parameters identified in received access requests as taught by Kikuchi because this guarantees for a plurality of information items to be processed, thus, can determine the restricting state to an access state of Rothermel.

As per claim 11:

Rothermal discloses a machine readable storage having stored thereon a computer program for permitting access to a network protected behind a stealth firewall, said computer program comprising a routine set of instructions for performing the steps of:

initializing a state machine configured to grant access to the stealth firewall contingent upon said state machine transitioning across a plurality of internal states (col.4, lines 35-45 and col.5, line 65 – col.6, line 2) *[responsive to receiving a plurality*

Art Unit: 2135

of requests to access the network from a single network device, said plurality of requests collectively comprising a code for causing said state machine to permit access to the network];

receiving an access request (**col.17, lines 23-28 and col.18, lines 3-8**) from a network device in a network which is external to the network protected behind the stealth firewall (**col.1, lines 30-35 and col.11, lines 18-38**), identifying an access parameter in said access request and transitioning from an initial state in said state machine to an intermediate state if said identified access request satisfies transitioning criteria associated with said state machine for transitioning from said initial state to said intermediate state;

receiving a further access request from said network device in said network which is external to the network protected behind the stealth firewall (**col.1, lines 23-35 and col.11, lines 18-38**), *[identifying a further access parameter in said further access request]* and transitioning from an intermediate state in said state machine to a final state if said identified further access request satisfies transitioning criteria associated with said state machine for transitioning from an intermediate state to said final state; (**col.8, lines 59-60 and col.13, lines 63-67**)

not providing a response to said network device upon receiving each said access request from said network device in said network which is external to the network protected behind the stealth firewall unless said network device provides a sequence of access requests to the stealth firewall causing said state machine to transition to said final state; and, (**col.5, lines 39-51 and col.9, lines 28-39**)

upon transitioning to said final state, permitting said network device to access the network protected behind the stealth firewall. **(col.16, lines 1-6 and col.17, lines 17-22)**

Rothermel teaches messages can include a variety of types of requests (col.18, lines 1-8), and further discloses gathering network security information of activities where it is analyzed during the process of protection from unauthorized access (col.5, lines 30-35 and 55-63). However, did not discuss in further details the gathering of security information that is responsive to receiving a plurality of requests to access the network from a single network device, said plurality of requests collectively comprising a code for causing said state machine to permit access to the network and identifying a further access parameter in said further access request.

Kikuchi an invention of transmitting and requesting access to documents on workstations through a network such as LAN (col.1, lines 12-15). Kikuchi discloses receiving a request for accessing information and analyzing the contents of the access request where the sequence of issued access requests are collectively reflected in the database as a single transaction (col.4, lines 15-22). In addition, when the client issues a sequence of access requests, the consistency is guaranteed for a plurality of information items to be process by the access requests (col.2, lines 62-65).

Hence, it would have been obvious for a person of ordinary skills in the art at the time of the invention to combine the method of receiving a plurality of requests to access the network from a single network device, said plurality of requests collectively comprising a code for causing said state machine to permit access to the network and identifying a further access parameter in said further access request as taught by

Art Unit: 2135

Kikuchi because this guarantees for a plurality of information items to be processed, thus, can determine the restricting state to an access state of Rothermel.

As per claim 12:

Rothermel discloses a machine readable storage having stored thereon a computer program for permitting access to a network protected behind a stealth firewall, said computer program comprising a routine set of instructions for performing the steps of:

[receiving a plurality of access requests] from a plurality of network devices which are external to the network protected behind the stealth firewall; **(col.1, lines 30-35 and col.11, lines 18-38)**

not providing a response to said plurality of network device upon receiving each of said access requests; **(col.5, lines 39-51 and col.9, lines 28-39)**

identifying access request parameters in said *[received access requests]*; **(col.5, line 63 – col.6, line 2)**

performing state transitions in a state machine in the stealth firewall based upon identifying particular ones of said identified access request parameters; and, **(col.13, lines 63-67 and col.17, lines 17-22)**

[upon identifying a pre-determined sequence of access request parameters, said identification of said sequence of access request parameters causing a corresponding sequence of state transitions in the said machine, permitting access to a selected network device responsible for transmitting said sequence of access requests parameters.]

Rothermel teaches messages can include a variety of types of requests (col.18, lines 1-8), and further discloses gathering network security information of activities where it is analyzed during the process of protection from unauthorized access (col.5, lines 30-35 and 55-63). However, did not discuss in further details the gathering of security information that is responsive to receiving a plurality of requests and upon identifying a pre-determined sequence of access request parameters, said identification of said sequence of access request parameters causing a corresponding sequence of state transitions in the said machine, permitting access to a selected network device responsible for transmitting said sequence of access requests parameters.

Kikuchi an invention of transmitting and requesting access to documents on workstations through a network such as LAN (col.1, lines 12-15). Kikuchi discloses receiving a request for accessing information and analyzing the contents of the access request where the sequence of issued access requests are collectively reflected in the database as a single transaction (col.4, lines 15-22). In addition, when the client issues a sequence of access requests, the consistency is guaranteed for a plurality of information items to be process by the access requests (col.2, lines 62-65).

Hence, it would have been obvious for a person of ordinary skills in the art at the time of the invention to combine the method of receiving a plurality of requests and upon identifying a pre-determined sequence of access request parameters, said identification of said sequence of access request parameters causing a corresponding sequence of state transitions in the said machine, permitting access to a selected network device responsible for transmitting said sequence of access requests

Art Unit: 2135

parameters as taught by Kikuchi because this guarantees for a plurality of information items to be processed, thus, can determine the restricting state to an access state of Rothermel.

As per claim 13:

Rothermel discloses a machine readable storage having stored thereon a computer program for permitting access to a network protected behind a stealth firewall, said computer program comprising a routine set of instructions for performing the steps of:

configuring a state machine to grant access to the stealth firewall (**col.1, lines 30-35 and col.11, lines 18-38**) contingent upon said state machine transitioning through a plurality of states *[based upon a sequence of access request parameters identified in received access requests from a single network device]*;

setting said sequence of access parameters to a specific set of access parameters; and, (**col.5, line 63 – col.6, line 2**)

disposing said state machine in the stealth firewall. (**col.12, lines 59-60**)

Rothermel teaches messages can include a variety of types of requests (col.18, lines 1-8), and further discloses gathering network security information of activities where it is analyzed during the process of protection from unauthorized access (col.5, lines 30-35 and 55-63). However, did not discuss in further details based upon a sequence of access request parameters identified in received access requests from a single network device.

Kikuchi an invention of transmitting and requesting access to documents on workstations through a network such as LAN (col.1, lines 12-15). Kikuchi discloses receiving a request for accessing information and analyzing the contents of the access request where the sequence of issued access requests are collectively reflected in the database as a single transaction (col.4, lines 15-22). In addition, when the client issues a sequence of access requests, the consistency is guaranteed for a plurality of information items to be process by the access requests (col.2, lines 62-65).

Hence, it would have been obvious for a person of ordinary skills in the art at the time of the invention to combine the method of based upon a sequence of access request parameters identified in received access requests from a single network device as taught by Kikuchi because this guarantees for a plurality of information items to be processed, thus, can determine the restricting state to an access state of Rothermel.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

5. Claims 10 is rejected under 35 U.S.C. 103(a) as being unpatentable over Rothermel, et al. (US 6,678,827), and further in view of Wiser, et al. (US 6,868,403).

As per claim 10:

Rothermel discloses a stealth firewall comprising:

a first network interface to an external network; **(col.1, lines 23-29)**

a second network interface to an internal network; **(col.1, lines 30-35 and col.11, lines 18-38)**

a packet filter for restricting access to said internal network **(col.3, lines 4-8 and col.4, lines 53-54)**, said packet filter ignoring requests from said external network to access said internal network; **(col.5, lines 14-17)**

fixed storage in which at least one authentication password can be stored; **(col.6, lines 60-62)**

However, Rothermel go into details of a hash processor configured to apply a hashing algorithm to said stored at least one authentication password and, a comparator configured to compare a hashed password and timestamp received from

Art Unit: 2135

said first network interface, with a hashed result produced by said hash processor for a stored password associated with a user at said first network interface, said comparator causing said packet filter to permit access to said internal network where said hashed password and timestamp matches said hashed result.

Wiser, et al. an invention relating to a secure online music distribution system over the Internet and provides for security of the media throughout the distribution system (col.3, lines 7-12). Further, Wiser teaches the authoring tool and the content manager cross authenticating each other wherein includes having a timestamp and a hash of the timestamp, the authoring tool username and password that is all encrypted with the content manager's private key. The hash is decrypted and then compares the two (col.12, lines 28-37). Therefore, it would have been obvious for a person of ordinary skills in the art at the time of the invention to combine the teaching of the hash timestamp and password and the hashed password and timestamp matches said hashed result as taught by Wiser with the teachings of a packet filter for restricting access to said internal network as taught by Rothermel is for security purposes because this ensures that the packet or message has not been altered and authorized.

Response to Arguments

In the Final office action (10/7/05), the examiner rejected claim 10 in view of Rothermel, et al. Claims 1-9 and 11-13 was previously rejected in view of Reid, et al. and have found applicant's arguments persuasive over Reid. Hence, only claim 10 will be addressed in regards to applicant's arguments. Claims 10 is now rejected as being unpatentable over Rothermel, et al. (US 6,678,827), and further in view of Wiser, et al. (US 6,868,403).

Rothermel did not go into details the hashing result wherein includes a hash password and timestamp and that the hashed password and timestamp matches to the hash result. Thus, the examiner brought forth an additional prior art to teach this limitation. Wiser, et al. an invention relating to a secure online music distribution system over the Internet and provides for security of the media throughout the distribution system (col.3, lines 7-12). Further, Wiser teaches the authoring tool and the content manager cross authenticating each other wherein includes having a timestamp and a hash of the timestamp, the authoring tool username and password that is all encrypted with the content manager's private key. The hash is decrypted and then compares the two which is applicant's hashed password and timestamp matches the hash result (col.12, lines 28-37). Therefore, it would have been obvious for a person a ordinary skills in the art at the time of the invention to combine the teaching of the hash timestamp and password and the hashed password and timestamp matches said hashed result as taught by Wiser with the teachings of a packet filter for restricting

access to said internal network as taught by Rothermel is for security purposes because this ensures that the packet or message authorized and has not been altered.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to LEYNNA T. HA whose telephone number is (571) 272-3851. The examiner can normally be reached on Monday - Thursday (7:00 - 5:00PM).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service


Application/Control Number: 09/944,996

Page 22

Art Unit: 2135

Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

LHa



KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100